McAfee Database Activity Monitoring

Экономичная система защиты баз данных для обеспечения нормативно-правового соответствия

В базах данных организаций хранятся самые ценные и конфиденциальные данные, однако средства защиты периметра и основной защиты баз данных не обеспечивают безопасность в случае сегодняшних изощренных атак злоумышленников или потенциальных угроз от недобросовестных внутренних пользователей. Как показывают исследования[1], более 96 % всего объема утечек информации произошли в результате взлома базы данных, а 66 % случаев взлома остаются необнаруженными на протяжении нескольких месяцев или дольше. McAfee® Database Activity Monitoring автоматически обнаруживает базы данных в вашей сети, обеспечивает их безопасность с помощью набора заранее сконфигурированных средств защиты и помогает создать специализированную политику безопасности для вашей среды, что упрощает декларирование нормативного соответствия при аудитах и повышает уровень защиты критически важных данных.

Ключевые преимущества

- Максимально повышает уровень визуального контроля и защиты от всех источников атак.
- Отслеживает внешние угрозы, угрозы со стороны привилегированных пользователей и изощренные атаки изнутри баз данных.
- Снижает уровень риска и ответственности за нарушения безопасности, поскольку останавливает атаку до того, как она может нанести ущерб.
- Экономит время и деньги благодаря ускоренному развертыванию и более эффективной архитектуре.
- Обеспечивает гибкость, позволяющую вам легко развернуть выбранную ИТ-инфраструктуру.
- Интегрируется с основными продуктами McAfee, такими как платформа управления McAfee® ePolicy Orchestrator® (McAfee ePO™) и McAfee Vulnerability Manager for Databases.

Решение McAfee Database Activity Monitoring позволит организациям получать информацию обо всех действиях, связанных с базами данных, включая локальный привилегированный доступ и изощренные атаки, организуемые изнутри базы данных. McAfee Database Activity Monitoring помогает обеспечить защиту наиболее ценных и конфиденциальных данных от внешних угроз и злоумышленных действий собственных сотрудников. Кроме создания достоверного журнала аудита решение McAfee Database Activity Monitoring также предотвращает вторжения, прерывая сеансы, которые нарушают политику безопасности.

McAfee Database Activity Monitoring, позволит организации:

- быстро создавать специализированную политику безопасности с целью обеспечения соответствия отраслевым требованиям или внутренним стандартам ИТ-управления;
- регистрировать в журнале необходимые для аудита события доступа к конфиденциальным данным, включая полную информацию об операциях;
- прерывать сеансы, нарушающие политики, и помещать в карантин подозрительных пользователей, тем самым предотвращая нарушение целостности данных;
- обеспечивать разделение обязанностей в соответствии с требованиями многих нормативов.

McAfee Database Activity Monitoring обеспечивает экономичную защиту ваших данных от всех угроз благодаря локальному мониторингу действий на каждом сервере баз данных, а также рассылке оповещений или пресечения вредоносных действий в реальном времени даже при работе в виртуальной или облачной среде.

Защита от всех типов угроз для баз данных

Атаки, направленные на ценные данные, хранящиеся в базах данных, могут исходить из сети, от локальных пользователей, зарегистрированных на самом сервере, и даже изнутри самой базы данных через хранимые процедуры или триггеры. McAfee Database Activity Monitoring использует датчики, расположенные в оперативной памяти, для улавливания всех трех типов угроз с помощью единого неинтрузивного решения. Затем эта информация может быть использована для декларирования соответствия нормативно-правовым требованиям при проведении аудитов и повышения общего уровня защиты наиболее ценных данных организации.

Выявление угроз по мере их возникновения. Снижение риска и ответственности

В отличие от базового аудита или анализа журналов событий, которые всего лишь сообщают о событиях постфактум, мониторинг и предотвращение вторжения в реальном времени позволяют блокировать нарушения до нанесения ущерба. Оповещения, включающие всю информацию о нарушении политики, направляются непосредственно на панель мониторинга для выполнения исправлений. Для обнаружения чрезвычайно опасных нарушений продукт может быть настроен на автоматическое прекращение подозрительных сеансов и помещение злоумышленников в карантин, что даст группе, осуществляющей защиту, время на расследование вторжения.

Виртуальное исправление обеспечивает защиту от известных средств использования уязвимостей и многих угроз «нулевого дня»

Не всегда имеется возможность немедленно установить исправления, полученные от поставщика базы данных, так как зачастую для установки исправлений необходимо протестировать приложения, а для установки обновлений — запланировать время простоя. Кроме того, в некоторых приложениях до сих пор используются более старые версии баз данных, для которых исправления больше не выпускаются. McAfee Database Activity Monitoring обнаруживает атаки, пытающиеся воспользоваться известными уязвимостями, а также распространенные направления угроз. Возможно выполнить настройку продукта, позволяющую либо направлять оповещения, либо прерывать сеансы в реальном времени. Виртуальные обновления для недавно обнаруженных уязвимостей предоставляются регулярно и могут быть реализованы без простоев базы данных, что обеспечивает защиту конфиденциальных данных до выпуска обновления поставщиком базы данных и установки обновления.

Быстрое и неинтрузивное развертывание при минимальном потреблении ресурсов

Будучи чисто программным продуктом, решение McAfee Database Activity Monitoring позволяет выполнить развертывание и приступить к защите баз данных менее, чем за час. Для дальнейшего ускорения развертывания McAfee Database Activity Monitoring автоматически проверяет наличие в сети баз данных и использует созданные мастером шаблоны обеспечения соответствия различным нормативно-правовым требованиям, направляя пользователя и помогая оперативно создавать специализированные политики безопасности для выполнения требований аудита. Распределяя ответственность в соответствии с политикой безопасности между независимыми датчиками, работающими на каждом сервере баз данных, McAfee Database Activity Monitoring эффективно снижает затраты, тем самым обеспечивая поддержку крупнейших предприятий.

Поддержка современной ИТ-инфраструктуры, включая виртуальные и облачные среды

Другие системы мониторинга баз данных полагаются на анализ сетевого трафика для выявления нарушений политики, что является либо невозможным, либо неэффективным в высокодинамичных и распределенных структурах, используемых для виртуализации центров обработки данных и облачных вычислений. Напротив, вы можете сконфигурировать датчики McAfee таким образом, чтобы они могли автоматически размещаться в каждой новой базе данных, запрашивать политику безопасности на основе хранимых данных и затем направлять оповещения на сервер управления. Даже в случае прерывания сетевого соединения данные все равно находятся под защитой, так как датчик внедряет политику безопасности локально, и оповещения попадают в очередь для доставки после того, как сервер снова станет доступен.

Интеграция с платформой McAfee ePolicy Orchestrator

Решение McAfee Database Activity Monitoring полностью интегрировано с программным обеспечением McAfee ePolicy Orchestrator, что обеспечивает централизованное формирование отчетов и сводную информацию обо всех ваших базах данных с консолидированной панели мониторинга. Программное обеспечение McAfee ePO может быть подключено к дополнительным защитным решениям McAfee, находящимися за пределами системы защиты баз данных, что даст вам единую панель мониторинга, позволяющую легко осуществлять управление средствами защиты и собирать всю необходимую информацию.

Решения McAfee для защиты баз данных

McAfee предлагает ряд решений для защиты баз данных, с помощью которых вы сможете получать полную информацию о общем состоянии и уровне защищенности ваших баз данных. Для получения более подробной информации посетите страницу www.mcafee.com/ru/products/database-security/index.aspx или же обратитесь либо к своему региональному представителю McAfee, либо к реселлеру McAfee.

О решениях McAfee для обеспечения безопасности конечных точек

Решения McAfee для обеспечения безопасности конечных точек обеспечивают безопасность всех ваших устройств, данных проходящих через эти устройства и приложений, установленных на устройствах. Наши комплексные и индивидуально настраиваемые решения снижают сложность, позволяя создать многоуровневую систему защиты конечных точек и при этом избежать падения производительности. Для получения подробной информации посетите страницу www.mcafee.com/ru/products/endpoint-protection/index.aspx.

[1] *Исследование компании Verizon Business* за 2013 г.

McAfee
An Intel Company

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.McAfee.ru

60603ds_dam_1013_fnl_ETMG